



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/982,203	10/18/2001	Gerd Breiter	DE920010053US1	7195

7590 01/26/2005

William Kinnaman, Jr.  
IBM Corporation  
Intellectual Property Law Department  
2455 South Road, M/S P386  
Poughkeepsie, NY 12601

EXAMINER

GELAGAY, SHEWAYE

ART UNIT	PAPER NUMBER
----------	--------------

2133

DATE MAILED: 01/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/982,203	BREITER ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Shewaye Gelagay	2133	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

**A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.**

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 18 October 2001.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-29 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-29 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                        | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)               | Paper No(s)/Mail Date. _____  |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>4/29/2002</u> .   | 6) <input type="checkbox"/> Other: _____                                    |

## DETAILED ACTION

1. Claims 1-29 have been examined.

### ***Claim Rejections - 35 USC § 103***

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

3. Claims 1-13 and 15-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Okamoto et al. United States Letters Patent Number 6,732,106 in view of Fung et al. United States Publication Number 2001/0052077.

As per claim 1:

Okamoto et al. teach a framework for controlling access rights to digital content in a distributed information system comprising:

first storage means for storing a reference to a user registered in said framework;  
(Col. 4, lines 65-67 and Col. 10, lines 14-15)

second storage means for storing a reference to digital content registered for said user; (Col. 6, lines 16-18) and,

Okamoto et al. do not explicitly disclose third storage means for storing a reference to a digital secure repository registered for said user, the digital secure repository containing storage means for storing a unique identifier and a reference to said digital content.

Fung et al. in analogous art, however, disclose storage means for storing a reference to a digital secure repository registered for said user, the digital secure repository containing storage means for storing a unique identifier and a reference to said digital content. (Page 1, paragraph 8; Page 3, paragraph 36; "digital secure repository" is interpreted as "universal mobile ID": -the interpretation is given based on the similarity of the functionality of the "digital secure repository" and the "universal mobile ID")

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Okamoto et al. to include storage means for storing a reference to a digital secure repository registered for said user, the digital secure repository containing storage means for storing a unique identifier and a reference to said digital content. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Fung et al. (Page 5, paragraph 7) in order to prevent an

Art Unit: 2133

authorized user from transferring to non-authorized users a key or other embodiments of a right that would allow the non-authorized users to access the for-pay content.

As per claim 2:

Okamoto et al. and Fung et al. teach all the subject matter as discussed above. In addition, Okamoto et al. further disclose a framework comprising: fourth storage means for storing a reference to a rendering device registered for said user. (Col. 4, lines 60-65)

As per claim 3:

Okamoto et al. and Fung et al. teach all the subject matter as discussed above. In addition, Fung et al. further disclose a framework comprising: a communication link for establishing communication to one or more of the set of said secure repository and said rendering device. (Page 1, paragraph 8, ...each client is associated with a universal mobile ID...)

As per claim 4:

Okamoto et al. and Fung et al. teach all the subject matter as discussed above. In addition, Fung et al. further disclose a framework wherein said secure repository further comprises storage means for storing a digital key for decrypting said digital content. (Page 4, paragraph 53 and Page 5, paragraph 54)

As per claim 5:

Okamoto et al. and Fung et al. teach all the subject matter as discussed above. In addition, Fung et al. further disclose a framework wherein said secure repository

Art Unit: 2133

further comprises storage means for storing a reference to a rendering device. (Page 1, paragraph 8)

As per claim 6:

Okamoto et al. and Fung et al. teach all the subject matter as discussed above.

In addition, Fung et al. further disclose a framework wherein said secure repository further comprises storage means for storing content rights for said digital content.

(Page 1, paragraph 8)

As per claim 7:

Okamoto et al. and Fung et al. teach all the subject matter as discussed above.

In addition, Fung et al. further disclose a framework wherein said secure repository further comprises storage means for storing a reference to said user. (Page 1, paragraph 8)

As per claim 8:

Okamoto et al. and Fung et al. teach all the subject matter as discussed above.

In addition, Fung et al. further disclose a framework wherein said secure repository further comprises a communication link for establishing communication to one or more of the set of said framework and said rendering device. (Page 1, paragraph 8; ...each client is associated with a universal mobile ID... ; Page 2, paragraph 15)

As per claim 9:

Okamoto et al. and Fung et al. teach all the subject matter as discussed above.

In addition, Okamoto et al. further disclose a framework wherein the framework is

Art Unit: 2133

realized as a set of web applications forming an Internet web site. (Col. 9, lines 42-43 and Col. 11, lines 16-18)

As per claim 10:

Okamoto et al. and Fung et al. teach all the subject matter as discussed above. In addition, Okamoto et al. further disclose an Internet web site offering a framework for controlling access rights to digital content in a distributed information system. (Col. 9, lines 44-47)

As per claim 11 and 17:

Okamoto et al. teach a method for controlling access rights to digital content in a distributed information system comprising the steps of:

registering a user with a framework for controlling access rights to digital content in said distributed information system; (Col. 12, lines 42-46)

registering digital content registered for said user. (Col. 13, lines 38-41)

Okamoto et al. do not explicitly disclose registering a digital secure repository registered for said user.

Fung et al. in analogous art, however, disclose registering a digital secure repository registered for said user. (Page 2, Paragraph 15)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Okamoto et al. to include storage means for storing a reference to a digital secure repository registered for said user, the digital secure repository containing storage means for storing a unique identifier and a reference to said digital content. This modification would have been

Art Unit: 2133

obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Fung et al. (Page 5, paragraph 7) in order to prevent an authorized user from transferring to non-authorized users a key or other embodiments of a right that would allow the non-authorized users to access the for-pay content.

As per claim 12:

Okamoto et al. and Fung et al. teach all the subject matter as discussed above. In addition, Okamoto et al. further disclose a method wherein registering a user further comprises the steps of: storing a reference to said user. (Col. 12, lines 65-67)

Fung et al. further disclose a method wherein registering a user further comprises the steps of:

receiving a message from said user comprising a reference to said digital secure repository; (Page 2, paragraph 15; ...a user accesses server content by first issuing a request to the server along with his UMID.)

validating said reference to said digital secure repository; (Page 2, paragraph 15)

As per claim 13:

Okamoto et al. and Fung et al. teach all the subject matter as discussed above. In addition, Okamoto et al. further disclose a method wherein registering a digital secure repository further comprises the steps of:

storing a reference to said issued digital secure repository and sending it to the user. (Col. 17, lines 14-15)

Fung et al. further disclose a method wherein registering a digital secure repository further comprises the steps of:



receiving a message from said user comprising credentials of the user; (Page 4, paragraph 45)

validating said credentials; (Page 4, paragraph 45)

if the credentials are valid, issuing a new digital secure repository; (Page 4, paragraph 45) and

As per claim 15:

Okamoto et al. and Fung et al. teach all the subject matter as discussed above. In addition, Okamoto et al. further disclose a method comprising the step of registering a rendering device for said user. (Col. 10, lines 15-17)

As per claim 16:

Okamoto et al. and Fung et al. teach all the subject matter as discussed above. In addition, Okamoto et al. further disclose a method wherein registering a rendering device further comprises the steps of:

receiving a message from said user comprising credentials of the user and a reference to said rendering device to be registered; (Col. 12, lines 6-8 and Col. 4, lines 62-65)

validating said credentials; (Col. 17, lines 54-56)

if the credentials are valid, storing the reference of the rendering device associated with said user. (Col. 10, lines 15-17)

4. Claims 14 and 18-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Okamoto et al. United States Letters Patent Number 6,732,106 in view of Fung et

Art Unit: 2133

al. United States Publication Number 2001/0052077 and further in view of Olson et al.

United States Publication Number US 2002/0003878.

As per claim 14:

Okamoto et al. and Fung et al. teach all the subject matter as discussed above.

In addition, Fung et al. further disclose a method wherein registering digital content further comprises the steps of:

receiving a message from said user comprising an order request and a reference to the user's digital secure repository; (Page 2, paragraph 15; ...a user accesses server content by first issuing a request to the server along with his UMID.)

validating said reference; (Page 2, paragraph 15)

if the reference is valid, performing purchase formalities; (Page 2, paragraph 15)

returning the encrypted document encryption key to the user and registering the purchased digital content for said user. (Page 2, paragraph 15)

Both references do not explicitly disclose encrypting the document encryption key associated with the requested digital content with the public key associated with said digital secure repository.

Olsen et al. in analogous art, however, disclose encrypting the document encryption key associated with the requested digital content with the public key associated with said digital secure repository. (Page 4, paragraph 54; ...a public key system is used to cipher the video decryption keys, ...)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Okamoto et al.

and Fung et al. to include encrypting the document encryption key associated with the requested digital content with the public key associated with said digital secure repository. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Olsen et al. (Page 5, paragraph 55) in order to protect the keys during transmission from Content Distribution Portal to the Rendering Device.

As per claim 18 and 25:

Okamoto et al. and Fung et al. all the subject matter as discussed above. In addition Okamoto et al. further teach a method for rendering digital content on a rendering device comprising the steps of:

receive a request for rendering digital content in a predetermined form;(Col.6 , lines 25-27)

reading information about access rights granted; (Col. 6, lines 28-35)

decrypting the document encryption key with the private key associated with said rendering device;(Col. 3, lines 57-58)

decrypting said digital content with said document encryption key; and rendering said digital content in the requested form. (Col. 2, lines 4-5 and Col. 3, line 61)

Both Okamoto et al. and Fung et al. do not explicitly disclose getting a document encryption key encrypted with the public key associated with said rendering device.

Olsen et al. in analogous art, however, disclose getting a document encryption key encrypted with the public key associated with said rendering device. (Page 4, paragraph 54; ...a public key system is used to cipher the video decryption keys, ...)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Okamoto et al. and Fung et al. to include encrypting the document encryption key associated with the requested digital content with the public key associated with said digital secure repository. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Olsen et al. (Page 5, paragraph 55) in order to protect the keys during transmission from Content Distribution Portal to the Rendering Device.

As per claim 19:

Okamoto et al., Fung et al. and Olsen et al. teach all the subject matter as discussed above. In addition, Okamoto et al. further disclose a method wherein the step of getting a document encryption key further comprises the steps:

determining from a storage device associated with said rendering device whether or not the digital content is bound to said rendering device and if yes receiving said document encryption key from said storage device. (Col. 6, lines 48 and lines 56-57)

As per claim 20:

Okamoto et al., Fung et al. and Olsen et al. teach all the subject matter as discussed above. In addition, Fung et al. further disclose a method wherein the step of getting a document encryption key further comprises the step of receiving said document encryption key from a digital secure repository. (Page 2, paragraph 15;...The user then decrypts the encrypted content using both his secret PIN and the content-specific key...)

As per claim 21:

Okamoto et al., Fung et al. and Olsen et al. teach all the subject matter as discussed above. In addition, Fung et al. further disclose a method wherein the step of reading from a digital secure repository further comprises the step of communicating with said digital secure repository over a communication link. (Page 1, paragraph 8, ...each client is associated with a universal mobile ID...)

As per claim 22:

Okamoto et al., Fung et al. and Olsen et al. teach all the subject matter as discussed above. In addition, Fung et al. further disclose a method wherein the step of reading from a digital secure repository further comprises the step of retrieving said digital secure repository from a storage device also keeping said digital content. (Page 4, paragraph 46)

As per claim 23:

Okamoto et al., Fung et al. and Olsen et al. teach all the subject matter as discussed above. In addition, Okamoto et al. further disclose a method wherein the step of decrypting said digital content further comprises the step of retrieving said digital content from a storage device. (Col. 2, lines 4-5 and Col. 3, line 61)

As per claim 24:

Okamoto et al., Fung et al. and Olsen et al. teach all the subject matter as discussed above. In addition, Okamoto et al. further disclose a method wherein the step of decrypting said digital content further comprises the step of retrieving said digital

Art Unit: 2133

content from over a communication link as downloaded or streaming data. (Col. 9, lines 50-58)

As per claim 26 and 27:

Okamoto et al. a method for binding digital content to a rendering device, the method comprising the following steps:

if binding is allowed according to the rights stored in said digital secure repository, receiving the respective document encryption key encrypted with the rendering device's public key, and storing the encrypted key for later decrypting the respective digital content. (Col. 6, lines 49-51 and Col. 6, line 55)

Okamoto et al. further disclose a communication means between the distribution server and the user device and checking distribution condition by comparing the number of digital data; of which the same consumer registered in the history data is authorized to receive the distribution, and the distribution condition information. (Col. 6, lines 28-35). In addition, Okamoto et al. teaches encrypting means for encrypting the decryption key using a key that is created based on the media ID received from the user device.

Okamoto et al. do not explicitly disclose establishing a connection from said rendering device to a digital secure repository; requesting from said digital secure repository digital content rights for specified digital content; and document encryption key encrypted with the rendering device's public key.

Fung et al. in analogous art, however, disclose

establishing a connection from said rendering device to a digital secure repository; (Page 1, paragraph 8, ...each client is associated with a universal mobile ID...)

requesting from said digital secure repository digital content rights for specified digital content. (Page 2, paragraph 15)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Okamoto et al. to include establishing a connection from said rendering device to a digital secure repository; requesting from said digital secure repository digital content rights for specified digital content. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Fung et al. (Page 2, paragraph 14) in order to assemble the digital material which is send to the client device by using the access information which is contained in the Universal Mobile ID.

Both references do not disclose document encryption key encrypted with the public key associated with said rendering device.

Olsen et al. in analogous art, however, disclose document encryption key encrypted with the public key associated with said rendering device. (Page 4, paragraph 54; ...a public key system is used to cipher the video decryption keys, ...)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Okamoto et al. and Fung et al. to include encrypting document encryption key associated with the

Art Unit: 2133

requested digital content with the public key associated with said digital secure repository. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Olsen et al. (Page 5, paragraph 55) in order to protect the keys during transmission from Content Distribution Portal to the Rendering Device.

As per claim 28 and 29:

Okamoto et al. teach a method for storing digital content from a rendering device onto a storage device, the method comprising the following steps:

if storing is allowed according to the rights stored in said digital secure repository, receiving the respective document encryption key encrypted with the respective public key of all rendering devices registered in said digital secure repository, and storing the encrypted keys together with said encrypted digital content on said storage device.

(Col. 3, lines 64-67 and Col. 6, lines 49-56 Col. 7, lines 23-34)

Okamoto et al. further disclose a communication means between the distribution server and the user device and checking distribution condition by comparing the number of digital data; of which the same consumer registered in the history data is authorized to receive the distribution, and the distribution condition information. (Col. 6, lines 28-35). In addition, Okamoto et al. teaches encrypting means for encrypting the decryption key using a key that is created based on the media ID received from the user device.

Okamoto et al. do not explicitly disclose establishing a connection from said rendering device to a digital secure repository; requesting from said digital secure



repository digital content rights for specified digital content; and document encryption key encrypted with the respective public key of all rendering devices.

Fung et al. in analogous art, however, disclose establishing a connection from said rendering device to a digital secure repository; (Page 1, paragraph 8, ...each client is associated with a universal mobile ID...)

requesting from said digital secure repository digital content rights for specified digital content. (Page 2, paragraph 15)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Okamoto et al. to include establishing a connection from said rendering device to a digital secure repository; requesting from said digital secure repository digital content rights for specified digital content. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Fung et al. (Page 2, paragraph 14) in order to assemble the digital material which is send to the client device by using the access information which is contained in the Universal Mobile ID.

Both references do not disclose document encryption key encrypted with the respective public key of all rendering devices.

Olsen et al. in analogous art, however, disclose document encryption key encrypted with the respective public key of all rendering devices. (Page 4, paragraph 54; ...a public key system is used to cipher the video decryption keys, ...)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Okamoto et al. and Fung et al. to include encrypting document encryption key associated with the requested digital content with the public key associated with said digital secure repository. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Olsen et al. (Page 5, paragraph 55) in order to protect the keys during transmission from Content Distribution Portal to the Rendering Device.

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Blumenthal U.S. No. 5784460

This reference pertains to a system for retrieving secured data from a storage device.

b. Takaragi et al. U.S. No. 5,117,458

This reference pertains to a secret information service system and method wherein an information service station enciphers information to be supplied by using an ID key for information destination subscribers.

c. Collard et al. U.S. No. 6,545,769

This reference pertains to a digital image reproduction apparatus.

d. Heaven et al. U.S. Pub. 2002018854

This reference pertains to using biometric information to control access to digital media that is obtained over a network such as the Internet.

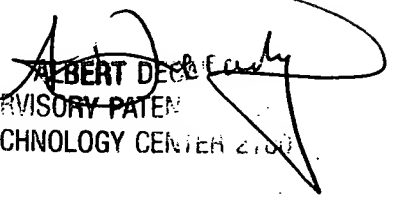
6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 571-272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay  
Examiner  
Art Unit 2133

01/07/05

  
ALBERT DECADY  
SUPERVISORY PATENT  
TECHNOLOGY CENTER 2100